Al-Hussein Ben Talal University

College of science

Department of mathematics

System of linear congruence

By

Mahmoud .Y Al-skafi

&

Malak .M Al-sheek Deeb

Supervised by:

Prof. Jehad .J Al-jaraden

A report submitted in partial fulfillment of the

requirement for the degree of Bachelor

Ma'an-Jordan

December 2019

الإهداء من ملاك محمود

مهما رسمنا جلالك أحرفاً قدسية تشدو بها الأرواح
فلأنت أعظم والمعاني كلها يارب عند جلالكم تنداح

بإسمك يا الله تشدو الألسن وتستغيث وتلهج وتنادي وبذكرك تطمئن القلوب وتسكن الأرواح وتهدلأ المشاعر وتبرد الأعصاب .

نجاحي وتخرجي وكل ما وصلت إليه بفضل الله أهديه لتلك الروح التي غادرتني منذ زمن والذي لطالما تمنيت وجودهم ، ذهبت أرواحهم وبقت ذكراهم السند الداعم لي بكل مراحل حياتي ، أبي عضيدي و أخي سندي استودع الله أرواحكم في كل ليلة

(أبي & أخي)

لتلك الروح التي كانت وما زالت الأم الداعمة بكل مراحل حياتي والتي لولا فضلها من بعد الله لما وصلت إلى ما انا عليه الأن أزاد الله في عمرك يا حبيبة .

(أمي الغالية)

إلى من كانوا معي في طريقي إلى النجاح ، إلى بلسم جراحي وسعادة أيامي .

(أخواني)

إلى صديقاتي اللواتي يحملن معنى أخواتي ، إلى من كانوا سر سعادتي ، إلى من كانوا معي في أحزاني وبسماتي .

(صديقاتي)

الإهداء من محمود يحيى

مهما رسمنا جلالك أحرفاً   قدسية تشدو بها الأرواح
فلأنت أعظم والمعاني كلها   يارب عند جلالكم تنداح

بإسمك يا الله تشدو الألسن وتستغيث وتلهج وتنادي وبذكرك تطمئن القلوب وتسكن الأرواح وتهدأ المشاعر وتبرد الأعصاب .

(أبي)

إلى من كانوا معي في طريقي إلى النجاح ، إلى بلسم جراحي وسعادة يا أبي.

(أمي الغالية)

الى الحب و الحنان و العطف و الامان الى ينبوع الصدق الصافي، الى من كان دعائها سر نجاحي و كلاهما دواءألامي ، الى أغلى الحبايب.

(أخواني)

إلى صديقاتي اللواتي يحملن معنى أخواتي ، إلى من كانوا سر سعادتي ، إلى من كانوا معي في أحزاني وبسماتي .

و أهدي روح الدكتور ابراهيم الفقي

قبل مضي ساعات الرحيل من الجميل ان نرجع الى اعوام تذكرنا كيف وصلنا الى هذه الساعات التي كانت هدف كل شخص يسعى اليها... ساعات الرحيل هي ساعاتٌ فضل قدومها يعود الى ربٍ كريم و أساتذةٍ كرام...

أساتذتي الكرام كل علمٍ تم أخذه ارتبط باسم أستاذ منكم فلكم منا كل آيات الشكر و الإمتنان و التقدير و المحبة و الإحترام على ما قدمتموه لنا...

سعيتم لبناء جيل بعد جيل و ها أنتم وصلتم إلى ما سعيتم فتحيةٌ منا مبطنةٌ بعطر الشكر و الإحترام يا حاملين رسالة العلم يا من تستحقون كلماتُ كلها تقدير الى اساتذتنا الأفاضل

أ.د. جهاد الجرادين   د. أحمد الحسنات   أ.د. علي العطيوي   أ.د. فراس الفقيه أ.د. عوني الدبابسة

د.سعدون العبيدي   د.أديب طلافحة   د. بلال الحسنات   د. إبراهيم جوارنه

د. أحمد عوجان   د. عايد العظامات   د. سحر القرالة   د. إيمان الصرايرة

د. سهم الطراونة   د. جهاد الحسنات   د. رمال الغنميين   د. سامي شكري

ونخص بالشكر والتقدير الأستاذ الدكتور جهاد البجرادين والدكتور أحمد الحسنات ...

استاذٌ علمنا ان نسعى وراء تحقيق ما هو هدفنا علمنا التفاؤل و الأمل علمنا ان بالعلم يصل الانسان .معلمٌ يستحق كلمة معلم بكل معانيها وقف إلى جانبنا عندما إحتجنا إلى من يرشدنا إلى الطريق انه الأستاذ الدكتور جهاد الجرادين الذي تفضل و قام بالإشراف على هذا البحث فجزاهُ الله عنا كل خير ووفقه بالسعي لنشر هذا العلم.

ولن ننسى بالشكر كل من اوصلنا الى هنا ووقف بجانبنا و أعطانا علماً حتى وإن كانت معلومة ونشكر كل من قام بإعطائنا أملاً و تفاؤلاً و معلومات وأفكار ومساعدات حتى إن لم يعلموا بذلك

نشكركم جميعاً

قدمتم لنا حصناً يحمينا من أيامٍ قادمةٍ لا نعلم ما فيها

Abstract

In this project, we study some important topics related to congruence in number theory framework. In particular, linear congruence, Chinese reminder theorem, and system of linear congruence are studied. To solve the system of linear congruence, we carry on the well-known methods that are used to deal with linear algebraic systems to give solutions of linear congruence systems. Such methods are Gauss-Jordan elimination and Crammer's rule. Non trivial solution of Homogeneous linear of congruence is found. Also, we re-define the modular matrix and the operation on it based on congruence, and investigates some properties for these matrices.

Contents

Introduction

Number theory is the study of the divisibility properties of the integers. Natural numbers are the oldest and the most fundamental mathematical objects. Since ancient time, human beings have been fascinated by magical, mystical properties of numbers. The numerous intriguing properties of numbers have led a great number of mathematicians and non- mathematicians to devote considerable energies to their study. The result has been the development a beautiful and powerful theory, whose aim is to answer questions about the integers. Our goal to study the elementary aspects of a wide array of techniques available to mathematicians.

In this project, we start by introducing congruences and their properties.

Chapter1

Congruence

The basic idea of congruences is to do arithmetic with the remainders obtained upon division by different integers. The reason being that all the information regarding divisibility questions is contained in the remainders obtained from divisions. The notation of congruences expresses the properties of remainders in a compact way, permitting their manipulation to deduce interesting facts about the integers. The notation and basic facts were given by Gauss in his great work, the Disquisitions Arithmetical published in 1801.

Definition 1.1.

If *a* and *b* are integers, we say that *a* **divides** *b* (a/b) if there exists an integer *c* such that $b = ac$. If no such *c* exists, then *a* dose not divides *b*. If *a* divides *b*, we say that *a* is **divisor** of *b*, and *b* is **divisible** by *a*.

Definition 1.2.

Let $m, a, and\ b$ be any integers, if *m* divides the difference $a - b$, then a and *b* are said to be **congruent** modulo *m*, that is, $a - b = km$ for some integer *k*. We use the notation *a* **congruent** *b* by $a \equiv b \pmod{m}$.

Example 1.1.

a) $12 \equiv 6 \pmod 2$, we say that $12\ is\ congruent$ 6 modulo 2 **because** $12-6=6, 2/6$.

b) $27 \equiv 9 \pmod 3$, we say that $27\ is\ congruent$ 9 modulo 3 **because** $27-9=18, 3/18$.

c) $16 \equiv 25 \pmod 3$, we say that $16\ is\ congruent$ 25 modulo 3 **because**$16-25=\ (-9), 3/\ (-9)$.

Definition 1.3.

Let *m* be a positive integer, the set of all equivalence classes modulo *m* is denoted by Z_m and is called the set of integers modulo *m*.

Example 1.2.

Let $m=3$, there are three equivalence classes for congruence modulo *3* so that the set $Z_3\ =\{[o],[1],[2]\}$ has three numbers.

Definition 1.4.

A number $\overline{a}$ is called the **invers of** *a* modulo *m* if $a\overline{a} \equiv \overline{a}a \equiv 1(\text{mod}\ m)$. We say that *a* is **invertible** modulo *m* if it has an inverse.

Remark.

We know that division is not defined in the set of integers modulo *m*. When we need to divide, we convert the divisor into multiplication in invers, i.e., if $b \neq 0\ and \gcd(b,m)=1$, then

$\frac{a}{b}$ modulo m is simply $a\bar{b}$, providing that b has an inverse $\bar{b}$ modulo m.

Example 1.3.

1) As $2 \cdot 6 \equiv 1(\text{mod } 11)$, the inverse of 6 modulo 11 is 2 and the inverse of 2 modulo 11 is 6.
2) The invers of 3 modulo 8 is 3 because $3 \cdot 3 \equiv 1(\text{mod } 8)$
3) There is no invers for 2 modulo 8, as $2x \equiv 1(\text{mod } 8)$ for some x implies that $8/2x - 1$, an impossibility, as $2x - 1$ is an odd number

Theorem 1.1.

The relation of congruence (≡) is an equivalence relation, that is,

1) Symmetric; $a \equiv a \ (\text{mod } m)$.
2) Reflexive; if $a \equiv b \ (\text{mod } m),\ then\ b \equiv a \ (\text{mod } m)$.
3) Transitive;
   if $a \equiv b \ (\text{mod } m)\ and\ b \equiv c(\text{mod } m), then\ \ a \equiv c \ (\text{mod } m),$ where a, b, and m are any integers.

Proof.

1) Since $m/(a - a) = 0$, it is easy to see that $a \equiv a(\text{mod } m)$.
2) If $a \equiv b(\text{mod } m)$, then $m/(a - b)$. Hence, there is an integer k with $km = a - b$. This shows that $(-k)m = b - a$, so that $m/(b - a)$. Consequently, $b \equiv a(\text{mod } m)$.
3) If $a \equiv b(\text{mod } m)\ \ and\ \ b \equiv c(\text{mod } m)$, then $m/(a - b)$ and $m/(b - c)$. Hence, there are integers $k\ and\ l$ with

$km = a - b$ and $lm = b - c$.Therefore, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$.Consequently, $m/(a - c)\ and\ a \equiv c(\text{mod}\ m)$ $\boxed{\text{Q.D.E}}$

Theorem 1.2.

If *a*, *b*, *c* and *m* are integers with $m > 0$ such that: $a \equiv b\ (\text{mod}\ m)$. Then:

a) $a + c \equiv b + c\ (\text{mod}\ m)$
b) $a - c \equiv b - c\ (\text{mod}\ m)$
c) $ca \equiv cb\ (\text{mod}\ m)$

Proof.

Since$a \equiv b(\text{mod}\ m)$, we know that $m/(a - b)$. From the identity $(a + c) - (b + c) = a - b$,we see

$m[(a + c) - (b + c)]$, so that (a)follows .Likewise,(b)follows from the fact that $(a - c) - (b - c) = a - b$.To show that (c) holds, note that $ac - bc = c(a - b)$.Since $m/(a - b)$,it follows that $m/c(a - b)$,and henece, $ac \equiv bc(\text{mod}\ m)$. $\boxed{\text{Q.D.E}}$

Example 1.4.

Since $19 \equiv 3(\text{mod}\ 8)$, it follows from Theorem 1.2 that $26 = 19 + 7 \equiv 3 + 7 = 10(\text{mod}\ 8)$, $15 = 19 - 4 \equiv 3 - 4 = -1(\text{mod}\ 8)$, and $38 = 19 \cdot 2 \equiv 3 \cdot 2 = 6(\text{mod}\ 8)$.

Theorem 1.3.

If a, b, c, d and m are integers such that $m > 0$, $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$. Then:

a) $a + c \equiv b + d \pmod{m}$
b) $a - c \equiv b - d \pmod{m}$
c) $ca \equiv bd \pmod{m}$

Proof.

Since $a \equiv b(\bmod\, m)$ *and* $c \equiv d(\bmod\, m)$, we know that $m/(a-b)$ *and* $m/(c-d)$. Hence, there are integers k *and* l with $km = a - b$ *and* $lm = c - d$.

To prove (a), note that

$(a+c) - (b+d) = (a-b) + (c-d) = km + lm = (k+l)m$.
Hence, $m/[(a+c) - (b+d)]$. Therefore, $a + c \equiv b + d \pmod{m}$.

To prove (b), note that

$(a-c) - (b-d) = (a-b) - (c-d) = km - lm = (k-l)m$.

Hence, $m/[(a-c) - (b-d)]$, *so that* $a - c \equiv b - d(\bmod\, m)$.

To prove (c), note that

$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-b) = ckm + blm = m(ck + bl)$. Hence, $m/(ac - bd)$. Therefore, $ac \equiv bd(\bmod\, m)$ $\boxed{\text{Q.D.E}}$

Example 1.5.

Since $13 \equiv 3(\bmod\, 5)$ and $7 \equiv 2(\bmod\, 5)$, using Theorem 1.3 we see that $20 = 13 + 7 \equiv 3 + 2 = 5(\bmod\, 5)$, $6 = 13 - 7 \equiv 3 - 2 = 1(\bmod\, 5)$, and $91 = 13 \cdot 7 \equiv 3 \cdot 2 = 6(\bmod\, 5)$

Chapter2

Linear congruence and Chinese reminder theorem.

2.1 linear congruence

Definition 2.1.1.

A congruence of the form

$$\boldsymbol{ax} \equiv \boldsymbol{b} \pmod{m}$$

Where x is an unknown integer, $\boldsymbol{ax} \equiv \boldsymbol{b} \pmod{m}$ is called a **linear congruence** in one variable.

In this section we will see that the study of such congruence similar to the study of linear Diophantine equations in two variables.

Theorem 2.1.1.

"Diophantine equations" Let a and b be positive integers with $d = gcd(a, b)$. The equation $ax + by = c$ has no integral solutions if d not factor c. lf d/c, then there are infinitely many integral solutions. Moreover, if $x = x_0,\ y = y_0$ is a particular solution of the equation, then all solutions are given by

$x = x_o + (b/a)t,\ y = y_o - (a/d)t$, where t is an integer.

Theorem 2.1.2.

"Linear congruence" Let *a*, *b* and *m* be integers with m>0, and $d = gcd(a, m)$. If *d* not factor *b*, then $ax \equiv b(\text{mod } m)$ has no solutions. If d/b, then $ax \equiv b$ (mod m) has exactly *d* incongruent solutions modulo *m*.

Proof.

From proposition "If a and b are integers, then $a \equiv b$ (mod m) if and only if there is an integer k such that $a = b + km$" the linear congruence $ax \equiv b$ (mod m) is equivalent to the linear diophantine equation in two variables $ax - my = b$. The integer x is a solution of $ax \equiv b$ (mod m) if and only if there is an integer y with $ax - my = b$. From Theorem 2.1.1, we know that if *d* not factor *b*, there are no solutions, while if $d\,/b\,, ax - my = b$ has infinitely many solutions, given by $x = x_o + (m/d)t, y = y_o - (a/d)t$. Where $x = x_o\ and\ y = y_o$ is a particular solution of the equation. The values of x given above, $x = x_o + (m/d)t$, are the solutions of the linear congruence; there are infinitely many of these.

To determine how many incongruent solutions there are, we find the condition that describes when two of the solution $x_1 = x_o + (m/d)t_1$ and $x_2 = x_o + (m/d)t_2$ are congruent modulo m. If these two solutions are congruent, then

$x_o + (m/d)t_1 \equiv x_o + (m/d)t_2(\text{mod } m)$.

Subtracting x_o from both sides of this congruence, we find that

$(m/d)t_1 \equiv (m/d)t_2(\text{mod } m)$.

Now $gcd(m, m/d) = m/d$ since $(m/d)/m$, so that

$$t_1 \equiv t_2(\text{mod } d)$$

This shows that a complete set of incongruent solutions is obtained by taking $x = x_o + (m/d)t$, where *t* ranges through a complete system of residues *modulo d*. One such set is given by $x = x_0 + (m/d)t$ where $t = 0,1,2, \dots, d-1$ $\boxed{\text{Q.D.E}}$

Example 2.1.1.

To find all solution of the linear congruence $9x \equiv 12 (\text{mod} 15)$. We first note that since $\gcd(9,15) = 3$ *and* $3/12$, there are exactly **three** incongruent solutions. We can find these solutions by first finding a particular solution and then adding the appropriate multiples of $15/3 = 5$.

To find a particular solution, we consider the linear Diophantine equation $9x - 15y = 12$. The Euclidean algorithm shows

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2, \end{aligned}$$

So that $3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15$. Hence, $9 \cdot 8 - 15 \cdot 4 + 12$, and a particular solution of $9x - 15y = 12$, is given by $x_0 = 8$ *and* $y_0 = 4$.

From the proof of Theorem 2.1.2, we see that a complete set of 3 incongruent solutions is given by $x = x_0 \equiv 8 \; (\text{mod } 15)$, $x = x_0 + 5 \equiv 13 (\text{mod } 15)$, and $x = x_0 + 5 \cdot 2 \equiv 18 \equiv 3 (\text{mod } 15)$

2.2 Chinese reminder theorem

An important problem is to find integers satisfying many different divisibility conditions. Also, in many applications, we reduce a computation modulo composite numbers to a computation over its prime factor. The Chinese Remainder Theorem is the fundamental tool that allows us to combine congruences to reach conclusion about the original problem. The idea first appears in the writings of the Chinese mathematician Sun-Tzu, who lived in the third century. The method was further developed by Chin Chiu-Shao in the thirteen century. In the west, Euler seems to have been the first to study it extensively. The method is fundamental and has numerous applications.

Chinese reminder theorem.

Let $m_1, m_2, \dots, m_r$ be pairwise relatively prime positive integer. Then the system of congruence

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

Has a unique solution modulo $M = m_1 m_2 \dots m_r$

proof

First, we construct a simultaneous solution to the system of congruence. To do this, let $M_k = M/m_k = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$. We know that $\gcd(M_k, m_k) = 1$ from "if $a_1, a_2, \dots, a_n$ are integers, and *b* is another integer such that $\gcd(a_1, b) = gcd(a_2, b) = \cdots = \gcd(a_n, b) = 1$, then $\gcd(a_1 a_2 \dots a_n, b) = 1$" since $\gcd(m_j, m_k) = 1$ whenever $j \neq k$. Hence, from Theorem 2.1.2, we can find an inverse $y_k$of M_k modulo m_k, so that $M_k\, y_k \equiv 1 (\text{mod } m_k)$. We now form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

The integer *x* is a simultaneous solution of the *r* congruences. To demonstrate this, we must show that $x \equiv a_k (\text{mod } m_k)$ for k=1,2,…,r. since m_k / M_kwhenever $j \neq k$ we have $M_j \equiv 0 (\text{mod } m_k)$. Therefore, in the sum for *x*, all terms except the kth term are congruent to $0 (\text{mod } m_k)$. Hence, $x \equiv a_k M_k y_k \equiv a_k (\text{mod } m_k)$, since $M_k\, y_k \equiv 1 (\text{mod } m_k)$. We now show that any two solutions are congruent modulo *M*. Let x_0 and x_1 both be simultaneous solutions to the system of *r* congruences. Then, for each *k*, $x_0 \equiv x_1 \equiv a_k (\text{mod } m_k)$, so that $m_k / (x_0 - x_1)$. Using Theorem 2.1.2, we see that $M / (x_0 - x_1)$. Therefore, $x_0 \equiv x_1 (\text{mod } M)$.This shows that the simultaneous solution of the system of *r* congruences is unique modulo *M*. $\boxed{\text{Q.D.E}}$

We illustrate the use of the Chinese remainder theorem by solving the system that arises from the ancient Chinese puzzle.

Example 2.2.1.

To solve the system

$$\begin{aligned} x &\equiv 1(\bmod 3) \\ x &\equiv 2(\bmod 5) \\ x &\equiv 3(\bmod 7) \end{aligned}$$

We have$M = 3 \cdot 5 \cdot 7 = 105, M_1 = 105/3 = 35,$

$M_2 = 105/5 = 21$, and $M_3 = 105/7 = 15$. To **determine** $y_{1,}$we solve $35y_1 \equiv 1(\text{mod } 3),$ equivalently, $2y_1 \equiv 1(\text{mod } 5)$.

This yield $y_1 \equiv 2(\text{mod } 3)$. We find y_2 by solving $35y_2 \equiv 1(\text{mod } 5)$; this immediately gives $y_2 \equiv 1(\text{mod } 5)$. Finally, we find $y_3$by solving$15y_3 \equiv 1(\text{mod } 7)$.This gives $y_3 \equiv 1(\text{mod } 7)$.Hence,

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1$$

$$\equiv 157 \equiv 52(\text{mod } 105)$$

Example 2.2.2.

To solve the linear congruence $9x \equiv 12(\text{mod}15)$ by using Chinese reminder theorem we first note that since $\gcd(9,15) = 3 \; and \; 3/12$, there exist *3* solutions. In this method we find one of them such that the primary factors of $15 = 3 \cdot 5$, so we can write the linear congruence as

$\begin{matrix} 9x \equiv 12(\text{mod}3) \\ 9x \equiv 12(\text{mod}5) \end{matrix}$, equivalently to $\begin{matrix} x \equiv 0(\text{mod}3) \\ x \equiv 3(\text{mod}5) \end{matrix}$.

Now, by using Chinese reminder theorem we have $M = 15$ $M_1 = 5$ and $M_2 = 3$.

To determine $y_{1,}$we solve $5y_1 \equiv 1(\text{mod } 3)$. This yield $y_1 \equiv 2(\text{mod } 3)$. Finally, we find $y_2$by solving $3y_2 \equiv 1(\text{mod } 5)$.This gives $y_2 \equiv 2(\text{mod } 5)$.Hence,

$$x \equiv 0 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2 \equiv 18 \equiv 3(\text{mod } 15)$$

Note that this method is not more effective than theorem 2.1.2, because finds any solution close to it, ignoring the other solutions, but it easier and faster when $\gcd(a, m) = 1$.

Example 2.2.3.

To solve the linear congruence $3x \equiv 4(\text{mod}10)$ by using Chinese reminder theorem we first note that since $\gcd(3{,}10) = 1 \; and \; 1/10$, there exists one solution. In this method we can find it such that the primary factors of $10 = 2 \cdot 5$, so we can write the linear congruence as

$\begin{matrix} 3x \equiv 4(\text{mod}2) \\ 3x \equiv 4(\text{mod}5) \end{matrix}$, equivalently to $\begin{matrix} x \equiv 0(\text{mod}2) \\ x \equiv 3(\text{mod}5) \end{matrix}$.

Now, by using Chinese reminder theorem we have $M = 10$ $M_1 = 5$ and $M_2 = 2$.

To determine $y_{1,}$we solve $5y_1 \equiv 1(\text{mod } 2)$. This yield $y_1 \equiv 1(\text{mod } 2)$. Finally, we find $y_2$by solving $2y_2 \equiv 1(\text{mod } 5)$.This gives $y_2 \equiv 3(\text{mod } 5)$.Hence,

$$x \equiv 0 \cdot 5 \cdot 1 + 3 \cdot 2 \cdot 4 \equiv 18 \equiv 8(\text{mod } 10)$$

Chapter 3

Modular matrix, Determent, Adjoint and Invers of modular matrix

3.1 modular matrix

Definition 3.1.1.

The matrix modulo *m* is called a ***modular matrix*** if its entries are the integers modulo *m*. We denoted by $\boldsymbol{A}$ (mod m) when $\boldsymbol{A}$ is the matrix over$\boldsymbol{Z_m}$.

In general

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} (\operatorname{mod} m)$$

Definition 3.1.2.

Let $A\ and\ B\ be\ n \times k$ modular matrices with integer entries, with$(i,j)th$ entries $a_{ij}\ and\ b_{ij}$, respectively. We say that *A* is **congruent** to *B* modulo *m* if $a_{ij} \equiv b_{ij}$ (mod m) for all pairs (i,j) with $1 \le i \le n$ and $1 \le j \le k$. We write $A \equiv B(\text{mod } m)$ if *A* is **congruent** to *B* modulo *m*.

Example 3.1.1.

We easily see that

$$\begin{bmatrix} 15 & 3 \\ 8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 4 & 3 \\ -3 & 1 \end{bmatrix} (\text{mod} 11)$$

Definition 3.1.3.

If A is an $m \times k$ modular matrix and B is an $k \times n$ modular matrix, then the ***product*** *AB* is the $m \times n$ modular matrix whose entries are determined as follows: To find the entry in row *i* and column *j* of *AB*, single out row *i* from the matrix *A* and column j from the matrix *B*. Multiply the corresponding entries from the row and column together, and then add up the resulting products

Proposition 3.1.1.

If A and B are $n \times k$ modular matrices with $A \equiv B(\text{mod } m)$, C is a $k \times p$ modular matrix and D is a $p \times n$ modular matrix, all with integer entries, then $AC \equiv BC(\text{mod } m)$ and $DA \equiv DB(\text{mod } m)$.

Proof.

Let the entries of A and B be a_{ij} *and* b_{ij}, respectively, for $1 \leq i \leq n$ and $1 \leq j \leq k$ and let the entries of C be c_{ij} for $1 \leq i \leq k$ and $1 \leq j \leq p$. The $(i,j)th$ entries of *AC* and *BC* are $\sum_{t=1}^{n} a_{it} c_{tj}$ and $\sum_{t=1}^{n} b_{it} c_{tj}$, respectively. Since $A \equiv B(\text{mod } m)$ we know that $a_{it} \equiv b_{it}(\text{mod } m)$ for all *i* and *k* Hence, from Theorem 1.3 we see that $\sum_{t=1}^{n} a_{it} c_{tj} \equiv \sum_{t=1}^{n} b_{it} c_{tj} (\text{mod } m)$. Consequently, $AC \equiv BC(\text{mod } m)$.

The proof that $DA \equiv DB(\text{mod } m)$ is similar and is omitted. Q.D.E

Example 3.1.2.

Consider the modular matrices

$$A=\begin{bmatrix}1&2&4\\2&1&0\end{bmatrix}(\text{mod}\,5), B=\begin{bmatrix}4&1&4&3\\0&4&3&1\\2&2&0&2\end{bmatrix}(\text{mod}\,5)\text{, find } AB.$$

Since A is a 2×3 modular matrix and B is a 3×4 modular matrix, the product AB is a 2×4 modular matrix. To determine, for example, the entry in row 2 and column 3 of AB, we single out row 2 from A and column 3 from B. Then, as illustrated below, we multiply corresponding entries together and add up these products.

$$\begin{bmatrix}1&2&4\\2&1&0\end{bmatrix}\begin{bmatrix}4&1&4&3\\0&4&3&1\\2&2&0&2\end{bmatrix}(\text{mod}\,5)=\begin{bmatrix}\#&\#&\#&\#\\\#&\#&1&\#\end{bmatrix}(\text{mod}\,5)$$

$$(2\cdot4+1\cdot3+0\cdot0)(\text{mod}\,5)=11(\text{mod}\,5)=1$$

The entry in row 1 and column 4 of AB is computed as follows:

$$\begin{bmatrix}1&2&4\\2&1&0\end{bmatrix}\begin{bmatrix}4&1&4&3\\0&4&3&1\\2&2&0&2\end{bmatrix}(\text{mod}\,5)=\begin{bmatrix}\#&\#&\#&3\\\#&\#&\#&\#\end{bmatrix}(\text{mod}\,5)$$

$$(1\cdot3+2\cdot1+4\cdot2)(\text{mod}\,5)=13(\text{mod}\,5)=3$$

The computations for the remaining entries are

$$(1\cdot4+2\cdot0+4\cdot2)(\text{mod}\,5)=12(\text{mod}\,5)=2$$
$$(1\cdot1+2\cdot4+4\cdot2)(\text{mod}\,5)=12(\text{mod}\,5)=2$$
$$(1\cdot4+2\cdot3+4\cdot0)(\text{mod}\,5)=10(\text{mod}\,5)=0$$
$$(2\cdot4+1\cdot0+0\cdot2)(\text{mod}\,5)=\ 8(\text{mod}\,5)=3$$
$$(2\cdot1+1\cdot4+0\cdot2)(\text{mod}\,5)=\ 6(\text{mod}\,5)=1$$
$$(2\cdot3+1\cdot1+0\cdot2)(\text{mod}\,5)=\ 7(\text{mod}\,5)=2$$

$$AB=\begin{bmatrix}2&2&0&3\\3&1&1&2\end{bmatrix}(\text{mod}\,5)$$

3.2 Determinants by Cofactor Expansion of modular matrix

In this section we will define the notion of a "determinant." This will enable us to give a specific formula for the inverse of an invertible modular matrix, whereas up to now we have had only a computational procedure for finding it. This, in turn, will eventually provide us with a formula for solutions of certain kinds of linear congruence.

Definition 3.2.1.

If *A* is an $n \times n$ modular matrix, then the ***minor*** of entry a_{ij} is denoted by M_{ij} and is defined to be the determinant of the submatrix that remains after the *ith* row and *jth* column are deleted from *A*. The number $(-1)^{i+j}M_{ij}$ is denoted by C_{ij} and is called the ***cofactor*** of entry a_{ij}.

Remark 1.

$$\text{the cofactor of modular matrix is} \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix} (\operatorname{mod} m)$$

Remark 2.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} (\operatorname{mod} m) = (a_{11}a_{22} - a_{12}a_{21})(\operatorname{mod} m)$$

Example 3.2.1.

Find the minors and cofactors for the modular matrix

$$A = \begin{bmatrix} 3 & 1 & 3 \\ 2 & 5 & 6 \\ 1 & 4 & 1 \end{bmatrix} (\text{mod}\, 7)$$

Solution

The minor of entry a_{11} is

$$M_{11} = \begin{vmatrix} 5 & 6 \\ 4 & 1 \end{vmatrix} = -19 (\text{mod}\, 7) = 2$$

The cofactor of a_{11} is

$$C_{11} = (-1)^{1+1} M_{11} = 2(\text{mod } 7) = 2$$

The minor of entry a_{12} is

$$M_{12} = \begin{vmatrix} 2 & 6 \\ 1 & 1 \end{vmatrix} = -4 (\text{mod}\, 7) = 3$$

The cofactor of a_{12} is

$$C_{12} = (-1)^{1+2} M_{12} = -3(\text{mod } 7) = 4$$

Similarly,

$$M_{13} = 3, M_{21} = 3, M_{22} = 0, M_{23} = 4, M_{31} = 5, M_{32} = 5 \, and \, M_{33} = 6$$
$$C_{13} = 3,\ C_{21} = 4,\ C_{22} = 0,\ C_{23} = 3,\ C_{31} = 5, C_{32} = 2 \text{ and } C_{33} = 6$$

$$\text{cofactor modular matrix of A} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & 0 & 3 \\ 5 & 2 & 6 \end{bmatrix} (\text{mod}\, 7)$$

Definition *3.2.2.*

If A is an $n \times n$ modular matrix, then the number obtained by multiplying the entries in any row or column of A by the corresponding cofactors and adding the resulting products is called the ***determinant of A***, and the sums themselves are called ***cofactor expansions of A***. That is,

$$\Delta \equiv det(A) \equiv \left(a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}\right) \text{ (mod } m)$$

[Cofactor expansions along *jth* column]

and

$$\Delta \equiv det(A) \equiv (a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}) \text{ (mod } m)$$

[Cofactor expansions along *ith* row]

Example *3.2.2.*

Find the determinant of the modular matrix

$A = \begin{bmatrix} 3 & 1 & 3 \\ 2 & 5 & 6 \\ 1 & 4 & 1 \end{bmatrix} (\text{mod}\,7)$, by cofactor expansion along the first row.

Solution

$$\Delta = \det(A) = \begin{vmatrix} 3 & 1 & 3 \\ 2 & 5 & 6 \\ 1 & 4 & 1 \end{vmatrix} = (3\begin{vmatrix} 5 & 6 \\ 4 & 1 \end{vmatrix} - 1\begin{vmatrix} 2 & 6 \\ 1 & 1 \end{vmatrix} + 3\begin{vmatrix} 2 & 5 \\ 1 & 4 \end{vmatrix})(\text{mod}\,7)$$

$$= (3(-19) - 1(-4) + 3(3))(\text{mod } 7)$$

$$= -44(\text{mod } 7) = 5$$

3.3 Adjoint of a modular matrix

In a cofactor expansion we compute $det(A)$ by multiplying the entries in a row or column by their cofactors and adding the resulting products. It turns out that if one multiplies the entries in any row by the corresponding cofactors from a *different* row, the sum of these products is always zero. (This result also holds for columns.) Although we omit the general proof, the next example illustrates the idea of the proof in a special case.

Definition 3.3.1.

The ***adjoint*** of $n \times n$ modular matrix A is the $n \times n$ modular matrix with $(i,j)th$ entryC_{ji}, where C_{ji} is $(-1)^{i+j}$ times the determinant of the modular matrix obtained by deleting the ith row and jth column from A. The **adjoint** of A is denoted by $\boldsymbol{adj}(\boldsymbol{A})$.

Example 3.3.1

Find the adjoint of the modular matrix

$$A = \begin{bmatrix} 3 & 1 & 3 \\ 2 & 5 & 6 \\ 1 & 4 & 1 \end{bmatrix} (\bmod 7)$$

Solution

The cofactors of A are

$$C_{11} = 2,\ \ C_{12} = 4,\ \ C_{13} = 3$$
$$C_{21} = 4,\ \ C_{22} = 0,\ \ C_{23} = 3$$
$$C_{31} = 5,\ \ C_{32} = 2,\ \ C_{33} = 6$$

The entire of $adj(A)$ is C_{ji} . Hence, the adjoint of A is

$$adj(A) = \begin{bmatrix} 2 & 4 & 5 \\ 4 & 0 & 2 \\ 3 & 3 & 6 \end{bmatrix} (\bmod 7) .$$

3.4 invers of modular matrix

Definition 3.4.1.

If $A\ and\ \overline{A}$ are $n \times n$ matrices of integers and if $\overline{\boldsymbol{A}}\boldsymbol{A} \equiv \mathbf{A}\overline{\mathbf{A}} \equiv \mathbf{I}(\text{mod } m)$, where

$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} (\bmod m)$ is the identity matrix of order n, then $\overline{A}$ is said to be an *inverse* of A modulo m.

Theorem 3.4.1.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} (\text{mod } m)$ be a modular matrix of integers, such that $\Delta = det\ A\ = ad - bc$ is relatively prime to the positive integer m. Then, **the modular matrix**

$$\overline{\boldsymbol{A}} = \overline{\Delta} \begin{bmatrix} \boldsymbol{d} & -\boldsymbol{b} \\ -\boldsymbol{c} & \boldsymbol{a} \end{bmatrix} (\textbf{mod } \boldsymbol{m})$$

Where $\overline{\Delta}$ is the inverse of Δ modulo m, is an **inverse** of A modulo m.

Proof.

To verify that the modular matrix $\overline{A}$ is an inverse of A modulo m, we need only verify that $A\overline{A} \equiv \overline{A}A \equiv I \ (\text{mod } m)$.

To see this, note that

$$A\overline{A} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \overline{\Delta} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv \overline{\Delta} \begin{bmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{bmatrix}$$

$$\equiv \overline{\Delta} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \overline{\Delta}\Delta & 0 \\ 0 & \overline{\Delta}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I(\text{mod}\, m)$$

and

$$\overline{A}A \equiv \overline{\Delta} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \overline{\Delta} \begin{bmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{bmatrix}$$

$$\equiv \overline{\Delta} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \overline{\Delta}\Delta & 0 \\ 0 & \overline{\Delta}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I(\text{mod}\, m),$$

Where $\overline{\Delta}$ is an inverse of $\Delta \ (\text{mod } m)$, which exists because $\gcd(\Delta, m) = 1$. $\boxed{\text{Q.D.E}}$

Theorem 3.4.2.

If A is an $n \times n$ matrix with $\det(A) \neq 0$, then

$$A \cdot adj(A) = \det(A) \cdot I$$

Using this theorem, for this theorem follows readily.

Theorem 3.4.3.

If A is an $n \times n$ modular matrix with integer entries and m is a positive integer such that $\gcd(\det A \ , m) = 1$, then the modular matrix $\overline{A} = \overline{\Delta} \ (adj(A))$ is an inverse of A modulo m, where $\overline{\Delta}$ is an inverse of $\Delta = \det A$ modulo m.

Proof.

If $gcd(det\ A, m) = 1$, then we know that $det\ A\ \neq 0$. Hence, from Theorem 3.4.2. We have

$$A \cdot adj\ A = (detA)I = \Delta I.$$

Since $gcd(detA, m) = 1$, there is an inverse $\overline{\Delta}$ of $\Delta =\ detA$ *modulo m.* Hence,

$$A\ (\overline{\Delta}\ adj\ A)\ \equiv\ A\ \cdot (adj\ A)\overline{\Delta} \equiv \Delta\overline{\Delta}\ I\ \equiv I(\text{mod}\ m),$$

and

$$\overline{\Delta}(adj\ A)A \equiv \overline{\Delta}(adj\ A \cdot A) \equiv \overline{\Delta}\Delta I \equiv I(\text{mod}\ m).$$

This shows that $\overline{A} = \overline{\Delta} \cdot\ (adj\ A)$ is an inverse of *A* modulo m. $\boxed{\text{Q.D.E}}$

Example 3.4.1.

Find the invers for the modular matrix

$$A = \begin{bmatrix} 3 & 1 & 3 \\ 2 & 5 & 6 \\ 1 & 4 & 1 \end{bmatrix} (\text{mod}\, 7).$$

Solution

Since $\Delta = \det(A) = 5$, $\gcd(5,7) = 1$ and $\overline{\Delta} = 3$ then the invers of *A* is

$$\overline{A} = 3\begin{bmatrix} 2 & 4 & 5 \\ 4 & 0 & 2 \\ 3 & 3 & 6 \end{bmatrix} (\text{mod}\, 7) = \begin{bmatrix} 5 & 5 & 1 \\ 5 & 0 & 6 \\ 2 & 2 & 4 \end{bmatrix} (\text{mod}\, 7)$$

Example 3.2.

For this modular matrix

$A = \begin{bmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{bmatrix} (\bmod 7)$, find:

a) $\Delta = \det A = -5 \ (\bmod 7) = 2(\bmod 7)$

b) $\overline{\Delta} = \overline{2}(\bmod 7) = 4(\bmod 7)$

c) $\textit{cofactor} \text{ of A} = \begin{bmatrix} 5 & 2 & 4 \\ 4 & 0 & 1 \\ 5 & 3 & 4 \end{bmatrix}$

d) $adj(A) = \begin{bmatrix} 5 & 4 & 5 \\ 2 & 0 & 3 \\ 4 & 1 & 4 \end{bmatrix} (\bmod 7)$

e) $\overline{A} = \overline{\Delta} \cdot adj(A) = 4 \cdot \begin{bmatrix} 5 & 4 & 5 \\ 2 & 0 & 3 \\ 4 & 1 & 4 \end{bmatrix} (\bmod 7) = \begin{bmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{bmatrix} (\bmod 7)$

Chapter 4

System of linear congruence

4.1 introduction to system of linear congruence

We will consider system of more than one congruences involving the same number of unknowns as congruences; where all congruences have the same modulus.

We begin our study with an example.

Suppose we wish to find all integers x and y such that both of the congruences.

$$3x + 4y \equiv 5(\text{mod}13)$$
$$2x + 5y \equiv 7(\text{mod}13)$$

Are satisfied. To attempt to find the unknowns x and y, we multiply the first congruence by 5 and the second by 4, to obtain.

$$15x + 20y \equiv 25(\text{mod}13)$$
$$8x + 20y \equiv 28(\text{mod}13)$$

We subtract the first and second, to find that

$$7x \equiv \ -3(\text{mod } 13)$$

Since 2 is an inverse of $7(\text{mod } 13)$, we multiply both sides of the above congruences by 2.This give

$$2 \cdot 7x \equiv 2 \cdot (-3)(\text{mod } 13)$$

This tells us that

$$x \equiv 7(\text{mod } 13)$$

Likewise, we can multiply the first congruence by 2 and the second by 3, to see that

$$6x + \ \ 8y \equiv 10(\bmod 13)$$
$$6x + 15y \equiv 21(\bmod 13)$$

When we subtract the first congruence from the second, we obtain

$$7y \equiv 11(\bmod 13)$$

To solve for y, we multiply both sides of this congruence by 2, an inverse of 7 modulo 13.We get

$$2 \cdot 7y \equiv 2 \cdot 11(\bmod 13)$$

So that

$$y \equiv 9(\bmod 13)$$

What we have shown is that any solution (x, y)must satisfy

$$x \ \equiv \ 7(\bmod 13), y \equiv 9(\bmod 13)$$

Theorem 4.1.1.

Let $a, b, c, d, e, f \ and\ m$ be integers with $m > 0$, such that $gcd(\Delta, m) = 1$, where $\Delta = ad - bc$. Then, the system of congruence

$$ax + by \equiv e\ (\bmod m)$$
$$cx + dy \equiv f\ \ (\bmod m)$$

Has a unique solution modulo m given by

$$x \equiv \overline{\Delta}(\mathrm{de} - \mathrm{bf})(\mathrm{mod\ m})$$
$$y \equiv \overline{\Delta}(\mathrm{af} - \mathrm{ce})(\mathrm{mod\ m})$$

Where $\overline{\Delta}$ is an inverse of Δ modulo *m*.

Proof.

We multiply the first congruence of the system by *d* and the second by *b*. to obtain

$$\mathrm{adx} + \mathrm{bdy} \equiv \mathrm{d}e\ (\mathrm{mod\ m})$$
$$\mathrm{bcx} + \mathrm{bdy} \equiv \mathrm{b}f\ (\mathrm{mod\ m})$$

Then, we subtract the second congruence from the first, to find that

$$(ad - bc)\, x \equiv de - bf \ (\text{mod } m),$$

Or, since $A = ad - bc,$

$$\Delta x \equiv de - bf \ (\text{mod } m\ ).$$

Next, we multiply both sides of this congruence by $\overline{\Delta}$, an inverse of Δ modulo *m*, to conclude that

$$x \equiv \overline{\Delta}(de - bf)\ (\text{mod } m)$$

In a similar way, we multiply the first congruence by *c* and the second by *a*, to obtain

$$\mathrm{acx} + \mathrm{bcy} \equiv \mathrm{c}e\ (\mathrm{mod\ m})$$
$$\mathrm{acx} + \mathrm{ady} \equiv \mathrm{a}f\ (\mathrm{mod\ m})$$

We subtract the first congruence from the second, to find that

$$(ad - bc)y \equiv af - ce(\text{mod } m)$$

or

$$\Delta y \equiv af - ce \pmod{m}.$$

Finally, we multiply both sides of the above congruence by $\overline{\Delta}$ to see that

$$y \equiv \overline{\Delta}(af - ce) \pmod{m}.$$

We have shown that if (x, y) is a solution of the system of congruences, then

$$x \equiv \overline{\Delta}(de - bf) \pmod{m}, y \equiv \overline{\Delta}(af - ce) \pmod{m}.$$

We can easily check that any such pair *(x,y)* is a solution. When

$x \equiv \overline{\Delta}(de - bf) \pmod{m}\ and\ y \equiv \overline{\Delta}(af - ce) \pmod{m}$, we have

$$\begin{aligned} ax + by &\equiv a\overline{\Delta}(de - bf) + b\overline{\Delta}(af - ce) \\ &\equiv \overline{\Delta}(ade - abf + abf - bce) \\ &\equiv \overline{\Delta}(ad - bc)e \\ &\equiv e \pmod{m}, \end{aligned}$$

and

$$\begin{aligned} cx + dy &\equiv c\overline{\Delta}(de - bf) + d\overline{\Delta}(af - ce) \\ &\equiv \overline{\Delta}(cde - bcf + adf - cde) \\ &\equiv \overline{\Delta}(ad - bc)f \\ &\equiv \overline{\Delta}\Delta f \\ &\equiv f \pmod{m} \end{aligned}$$

This establishes the theorem $\boxed{\text{Q.D.E}}$

Example 4.1.1

Solve the system of linear congruence

$$3x + 4y \equiv 5(\text{mod}13)$$
$$2x + 5y \equiv 7(\text{mod}13)$$

Solution

By using theorem 4.1.1, we have;

$\Delta = 3 \cdot 5 - 4 \cdot 2 = 7, \text{gcd}(7{,}13) = 1$

$\overline{\Delta} = \overline{7}(\text{mod } 13) = 2$

$$\text{x} \equiv 2(5 \cdot 5 - 4 \cdot 7)(\text{mod}13)$$
$$\text{y} \equiv 2(3 \cdot 7 - 2 \cdot 5)(\text{mod}13)$$

Then,

$$x \equiv 7(\text{mod}13)$$
$$y \equiv 9(\text{mod}13)$$

Now let us consider **the system of congruence's**

$$\begin{aligned} &\text{a}_{11}\text{x}_1 + \text{a}_{12}\text{x}_2 + \ \dots \ + \text{a}_{1\text{n}}\text{x}_\text{n} \equiv \text{b}_1 \ (\text{mod m}) \\ &\text{a}_{21}\text{x}_1 + \text{a}_{22}\text{x}_2 + \ \dots \ + \text{a}_{2\text{n}}\text{x}_\text{n} \equiv \text{b}_2 \ (\text{mod m}) \\ &\qquad\qquad\quad \vdots\vdots\vdots \\ &\text{a}_{\text{n}1}\text{x}_1 + \text{a}_{\text{n}2}\ \text{x}_\text{n} + \ \dots \ + \text{a}_{\text{nn}}\text{x}_\text{n} \equiv \text{b}_\text{n} (\text{mod m}) \end{aligned}$$

Using modular matrix notation, we see that this system of n congruence's is equivalent to the modular matrix congruence $\boldsymbol{AX} \equiv \boldsymbol{B}(\text{mod } m)$,

$$\text{where } A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} (\bmod m), X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} (\bmod m); and, B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} (\bmod m).$$

4.2 solving the system of liner congruence

We now develop a method for solving congruence of the form $\boldsymbol{AX} \equiv \boldsymbol{B}(\text{mod } m)$. This method is based on finding a modular matrix $\overline{\boldsymbol{A}}$ such that$\overline{\boldsymbol{A}}\,\boldsymbol{A} \equiv \boldsymbol{I}(\text{ mod } m)$, where **I** is the identity modular matrix.

Theorem 4.2.1.

If *A* is an invertible *n*×*n* modular matrix, then for each *n*×*1* modular matrix ***B***, the system of linear congruence $\boldsymbol{AX} \equiv \boldsymbol{B}(\text{mod } m)$ has exactly one solution, namely $\boldsymbol{X} \equiv \overline{\boldsymbol{A}} \cdot \boldsymbol{B}(\text{mod } m)$.

Proof.

Since $A(\overline{A} \cdot b) \equiv (A \cdot \overline{A})b \equiv b(\text{mod } m)$, it follows that $\boldsymbol{X} \equiv \overline{\boldsymbol{A}} \cdot \boldsymbol{b}(\text{mod } m)$ is a solution of $\boldsymbol{AX} \equiv \boldsymbol{B}(\text{mod } m)$. To show that this is the only solution, we will assume that x_0 is an arbitrary solution and then show that x_0 must be the solution $\overline{\boldsymbol{A}} \cdot \boldsymbol{B}(\text{mod } m)$.

If x_0 is any solution, then $Ax_0 \equiv B(\text{mod } m)$.Multiplying both sides by $\overline{\boldsymbol{A}}$, we obtain $x_0 \equiv \overline{A} \cdot B(\text{mod } m)$. $\boxed{\text{Q.D.E}}$

Example 4.2.1.

Solve the system of linear congruence

$$\begin{aligned} 2x+3y+\ \ z &\equiv 3 \pmod 5 \\ x+2y+3z &\equiv 1 \pmod 5 \\ 3x+2y+\ \ z &\equiv 1 \pmod 5 \end{aligned}$$

Solution

We convert the system as modular matrix notation

$$\begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix} (\text{mod} 5)$$

We find determent of modular matrix A

$\Delta = det(A) = 12(\text{mod } 5) = 2$

$\overline{\Delta} = 3$

$\gcd(\Delta, m) = 1, \text{"}relatively\ prime\text{"}$

$$\overline{A} = \begin{bmatrix} 3 & 2 & 1 \\ 4 & 2 & 0 \\ 3 & 0 & 3 \end{bmatrix} (\text{mod} 5)$$

By using Theorem 4.2.1, $\boldsymbol{X} \equiv \overline{\boldsymbol{A}}\,\boldsymbol{B}(\text{mod } m)$. Hence

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 & 2 & 1 \\ 4 & 2 & 0 \\ 3 & 0 & 3 \end{bmatrix}\begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix} (\text{mod} 5)$$

$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 4 \\ 2 \end{bmatrix} (\text{mod} 5)$. Hence;

$$x \equiv 2 \pmod 5$$
$$y \equiv 4 \pmod 5$$
$$z \equiv 2 \pmod 5$$

4.3 The Gauss-Jordan elimination for solving system of liner congruence

In this section we will develop a systematic procedure for solving systems of linear congruence. The procedure is based on the idea of performing certain operations on the rows of the augmented modular matrix for the system that simplifies it to a form which the solution of the system can be ascertained by inspection

The **Gauss-Jordan** reduction procedure for solving the system of linear congruence $\boldsymbol{AX} \equiv \boldsymbol{B} (\text{mod } m)$ is as follows.

Step 1. Form the augmented modular matrix $[A \ \vdots \ B] (\text{mod} \, m)$.

Step 2. Transform the augmented modular matrix to reduced row echelon form by using elementary row operations modulo *m*.

Step 3. The system of linear congruence that corresponds to the modular matrix in reduced row echelon form that has been obtained in *step 2* has exactly the same solutions as the given system of linear congruence. For each nonzero row of the modular matrix in reduced row echelon form, solve the corresponding equation for the unknown that corresponds to the leading entry of the row. The rows consisting entirely of zeros can be ignored, since the corresponding linear congruence will be satisfied for any values of the unknowns.

Example 4.3.1.

Solve the system of linear congruence

$$\begin{aligned} 2x+3y+\ \ z &\equiv 3 \pmod 5) \\ x+2y+3z &\equiv 1 \pmod 5) \\ 3x+2y+\ \ z &\equiv 1 \pmod 5) \end{aligned}$$

By using Gauss-Jordan elimination method.

Solution.

Step 1. The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 2 & 3 & 1 & \vdots & 3 \\ 1 & 2 & 3 & \vdots & 1 \\ 3 & 2 & 1 & \vdots & 1 \end{bmatrix} (\text{mod}\, 5).$$

Step 2. We now transform the modular matrix in *step 1* to get it in the reduced row echelon form as follows:

We multiply the first row by $\overline{2}(\text{mod } 5) = 3$ to have 1 in the leading element position. This gives

$$\begin{bmatrix} 1 & 4 & 3 & \vdots & 4 \\ 1 & 2 & 3 & \vdots & 1 \\ 3 & 2 & 1 & \vdots & 1 \end{bmatrix} (\text{mod}\, 5).$$

We multiply the first row by $-1(\text{mod } 5) = 4$ and add the resulted row to the second one. Also, we multiply the first row by $-3(\text{mod } 5) = 2$ and add to the third row to obtain

$$\begin{bmatrix} 1 & 4 & 3 & \vdots & 4 \\ 0 & 3 & 0 & \vdots & 2 \\ 0 & 0 & 2 & \vdots & 4 \end{bmatrix} (\text{mod}\, 5).$$

In the last new matrix, we multiply the second row by $\overline{3}(\text{mod } 5) = 2$ to obtain

$$\begin{bmatrix} 1 & 4 & 3 & \vdots & 4 \\ 0 & 1 & 0 & \vdots & 4 \\ 0 & 0 & 2 & \vdots & 4 \end{bmatrix} (\mathrm{mod}\, 5)\,.$$

Then, we multiply the second row by $-4(\text{mod } 5) = 1$ and add the resulted row to the first row so that we get

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 3 \\ 0 & 1 & 0 & \vdots & 4 \\ 0 & 0 & 2 & \vdots & 4 \end{bmatrix} (\mathrm{mod}\, 5)..$$

Now, we multiply the third row by $\overline{2}(\text{mod } 5) = 3$ to have 1 in the leading element position of the third row. This leads to

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 3 \\ 0 & 1 & 0 & \vdots & 4 \\ 0 & 0 & 1 & \vdots & 2 \end{bmatrix} (\mathrm{mod}\, 5)..$$

We multiply now the third row by $-3(\text{mod } 5) = 2$ and add to the first row to obtain

$$\begin{bmatrix} 1 & 0 & 0 & \vdots & 2 \\ 0 & 1 & 0 & \vdots & 4 \\ 0 & 0 & 1 & \vdots & 2 \end{bmatrix} (\mathrm{mod}\, 5)..$$

Step 3. The system of linear congruence represented the *step 2* is

$$\begin{aligned} x &\equiv 2(\mathrm{mod}\, 5) \\ y &\equiv 4(\mathrm{mod}\, 5) \\ z &\equiv 2(\mathrm{mod}\, 5) \end{aligned}$$

4.4 Cramer's rule for the system of liner congruence

Cramer's Rule The next theorem provides a formula for the solution of certain system of linear congruence of n equations in n unknowns. This formula, known as **Cramer's Rule** is of marginal interest for computational purposes, but it is useful for studying the mathematical properties of a solution without the need for solving the system.

Theorem 4.4.1.

"Cramer's Rule" If $AX \equiv b (\text{mod } m)$ is a system of linear congruence in n unknowns such that $detA \neq 0$ and $\gcd(\det(A), m) = 1$, then the system of linear congruence has a unique solution. This solution is

$$\begin{aligned} x_1 &\equiv \overline{\Delta} \cdot \det(A_1) (\text{mod}\, m) \\ x_2 &\equiv \overline{\Delta} \cdot \det(A_2) (\text{mod}\, m) \\ &\vdots \\ x_n &\equiv \overline{\Delta} \cdot \det(A_n) (\text{mod}\, m). \end{aligned}$$

Where A_j is the modular matrix obtained by replacing the entries in the j^{th}column of A by the entries in the modular matrix

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} (\text{mod}\, m)$$

Proof.

If $detA \neq 0$ and $\gcd(\det(A), m) = 1$, then *A* is invertible and, by Theorem 4.2.1, $\boldsymbol{X} \equiv \overline{\boldsymbol{A}} \cdot \boldsymbol{b} (\text{mod } m)$ is the unique solution of $\boldsymbol{AX} \equiv \boldsymbol{b} (\text{mod } m)$. Therefore, by Theorem 3.4.3, we have

$$X \equiv \overline{A} \cdot b \equiv \overline{\Delta} \cdot adj(A) \cdot b \equiv \overline{\Delta} \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} (\text{mod}\, m)$$

Multiplying the matrices out gives

$$X \equiv \overline{\Delta} \begin{bmatrix} b_1 C_{11} + b_2 C_{21} + \cdots + b_n C_{n1} \\ b_1 C_{12} + b_2 C_{22} + \cdots + b_n C_{n2} \\ \vdots \quad\quad \vdots \quad\quad\quad\quad \vdots \\ \mathrm{b}_1 C_{1n} + b_2 C_{2n} + \cdots + b_n C_{nn} \end{bmatrix} (\text{mod}\, m)$$

The entry in the j^{th} row of *x* is therefore

$$x_j = \overline{\Delta}(b_1 C_{1j} + b_2 C_{2j} + \cdots + b_n C_{nj})$$

Now let

$$A_j \equiv \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j-1} & b_1 & a_{1j+1} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j-1} & b_2 & a_{2j+1} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nj-1} & b_n & a_{nj+1} & \cdots & a_{nn} \end{bmatrix} (\text{mod}\, m)$$

Since A_j differs from *A* only in the j^{th}column, it follows that the cofactors of entries $b_1, b_2, \cdots, b_n$ in A_j are the same as the cofactors of the corresponding entries in the j^{th} column of *A*. cofactors expansion of $det(A_j)$ along the j^{th}column is therefor $det(A_j) \equiv (b_1 C_{1j} + b_2 C_{2j} + \cdots + b_n C_{nj})$ $(\text{mod } m)$.Then,

$$x_j \equiv \overline{\Delta}\, det(A_j) \qquad \boxed{\text{Q.D.E}}$$

Example 4.4.1

Solve the system of linear congruence

$$\begin{aligned} 2x+3y+\ \ z &\equiv 3(\text{mod } 5) \\ x+2y+3z &\equiv 1(\text{mod } 5) \\ 3x+2y+\ \ z &\equiv 1(\text{mod } 5) \end{aligned}$$

By using crammer's rule

Solution

$\Delta = det(A) = 12(\text{mod } 5) = 2$

$\overline{\Delta} = 3$

$$\overline{A} = \begin{bmatrix} 3 & 2 & 1 \\ 4 & 2 & 0 \\ 3 & 0 & 3 \end{bmatrix} (\text{mod} 5)$$

Now, by using Theorem 4.4.1 the solution is

$$A_1 = \begin{bmatrix} 3 & 3 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 1 \end{bmatrix} (\text{mod} 5), \det(A_1) = -6(\text{mod} 5) = 4$$

$$A_2 = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 1 & 3 \\ 3 & 1 & 1 \end{bmatrix} (\text{mod} 5), \det(A_2) = 18(\text{mod} 5) = 3$$

$$A_3 = \begin{bmatrix} 2 & 3 & 3 \\ 1 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix} (\text{mod} 5), \det(A_3) = -6(\text{mod} 5) = 4$$

$$\begin{aligned} x &\equiv 3\cdot 4(\bmod 5) \equiv 2(\bmod 5) \\ y &\equiv 3\cdot 3(\bmod 5) \equiv 4(\bmod 5) \\ z &\equiv 3\cdot 4(\bmod 5) \equiv 2(\bmod 5) \end{aligned}$$

4.5 The system of linear congruence with finitely many solutions

Definition 4.5.1.

If a linear system of congruence has finitely many solutions, then a set of parametric equations from which all solutions can be obtained by assigning numerical values to the parameters is called a ***general solution*** of the system.

Example 4.5.1.

Solve the system of linear congruence

$$\begin{aligned} x + \ \ y + \ \ z &\equiv 1(\bmod 5) \\ 2x + 4y + 3z &\equiv 1(\bmod 5) \end{aligned}$$

Solution

By using Gauss-Jordan method we have

The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 1 & 1 & 1 & \vdots & 1 \\ 2 & 4 & 3 & \vdots & 1 \end{bmatrix} (\bmod 5). \ .$$

Reducing this modular matrix to reduced row-echelon modulo 5 form

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 4 \\ 0 & 1 & 3 & \vdots & 2 \end{bmatrix} (\bmod 5)..$$

The corresponding system of linear congruence is

$$\begin{aligned} x \quad + 3z &\equiv 4(\bmod 5) \\ y + 3z &\equiv 2(\bmod 5) \end{aligned}$$

Solving for the leading variable, we obtain

$$\begin{aligned} x &\equiv 4 + 2z(\bmod m) \\ y &\equiv 2 + 2z(\bmod m) \end{aligned}$$

Now, if we assign the free variable z arbitrary value t in Z_5, the *general solution* is given by the formulas

$$\begin{aligned} x &\equiv 4 + 2t(\bmod 5) \\ y &\equiv 2 + 2t(\bmod 5) \\ z &\equiv \quad\ t(\bmod 5) \end{aligned}.$$

For each t in Z_5; $t = \{0,1,2,3,4\}$, there exist a solutions such that

If $t = 0$, then:

$$\begin{aligned} x &\equiv 4(\bmod 5) \\ y &\equiv 2(\bmod 5) \\ z &\equiv 0(\bmod 5) \end{aligned}$$

If $t = 1$, then:

$$\begin{aligned} x &\equiv 1(\bmod 5) \\ y &\equiv 4(\bmod 5) \\ z &\equiv 1(\bmod 5) \end{aligned}$$

If $t = 2$, then:

$$x \equiv 3 \pmod 5$$
$$y \equiv 1 \pmod 5$$
$$z \equiv 2 \pmod 5$$

If $t = 3$, then:

$$x \equiv 0 \pmod 5$$
$$y \equiv 3 \pmod 5$$
$$z \equiv 3 \pmod 5$$

If $t = 4$, then:

$$x \equiv 2 \pmod 5$$
$$y \equiv 0 \pmod 5$$
$$z \equiv 4 \pmod 5$$

Example 4.5.2.

Solve the system of linear congruence

$$\begin{aligned} x + 3y + \ z &\equiv 4 \pmod 5 \\ x + \ y + 4z &\equiv 1 \pmod 5 \\ 3x + \ y \qquad &\equiv 0 \pmod 5 \end{aligned}$$

Solution

By using Gauss-Jordan elimination method we have

The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 1 & 3 & 1 & \vdots & 4 \\ 1 & 1 & 4 & \vdots & 1 \\ 3 & 1 & 0 & \vdots & 0 \end{bmatrix} \pmod 5 . .$$

Reducing this modular matrix to reduced row-echelon modulo 5 form

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 2 \\ 0 & 1 & 1 & \vdots & 4 \\ 0 & 0 & 0 & \vdots & 0 \end{bmatrix} (\mathrm{mod}\,5)..$$

The corresponding system of linear congruence is

$$\begin{aligned} x \quad + 3z &\equiv 2(\mathrm{mod}\,5) \\ y + \quad z &\equiv 4(\mathrm{mod}\,5) \end{aligned}$$

Solving for the leading variable, we obtain

$$\begin{aligned} x &\equiv 2 + 2z(\mathrm{mod}\,5) \\ y &\equiv 4 + 4z(\mathrm{mod}\,5) \end{aligned}$$

Now, if we assign the free variable z arbitrary value t in Z_5, the *general solution* is given by the formulas

$$\begin{aligned} x &\equiv 2 + 2t(\mathrm{mod}\,5) \\ y &\equiv 4 + 4t(\mathrm{mod}\,5) \\ z &\equiv \qquad t(\mathrm{mod}\,5) \end{aligned}$$

Then the system of linear congruence has finitely many solutions such as: since $t = 0$, then

$$\begin{aligned} x &\equiv 2(\mathrm{mod}\,5) \\ y &\equiv 4(\mathrm{mod}\,5) \\ z &\equiv 0(\mathrm{mod}\,5). \end{aligned}$$

4.6 The system of linear congruence with no solution

Example 4.6.1.

Solve the system of linear congruence

$$\begin{aligned} x+2\mathrm{y}+\ z &\equiv 2\,(\bmod 5) \\ 2x+3y+3z &\equiv 1\,(\bmod 5) \\ x+2y+\ z &\equiv 4\,(\bmod 5) \end{aligned}$$

Solution

By using Gauss-Jordan elimination method we have

The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 1 & 2 & 1 & \vdots & 2 \\ 2 & 3 & 3 & \vdots & 1 \\ 1 & 2 & 1 & \vdots & 4 \end{bmatrix}(\bmod 5)..$$

Reducing this modular matrix to reduced row-echelon modulo 5 form

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 1 \\ 0 & 1 & 4 & \vdots & 3 \\ 0 & 0 & 0 & \vdots & 2 \end{bmatrix}(\bmod 5)..$$

The system of linear congruence has no solution since 0 not congruent to 2 modulo 5.

4.7 Homogeneous linear system of congruence

A system of linear congruence is side to be homogeneous if it the constant terms are all (zero or *m*); that is, the system of congruence has the form

$$\begin{gathered}a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \equiv 0 \pmod m) \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \equiv 0 \pmod m) \\ \ldots \\ a_{n1}x_1 + a_{n2}x_n + \ldots + a_{nn}x_n \equiv 0 \pmod m).\end{gathered}$$

Every homogeneous system of linear congruence is consistent, since all such systems have $x_1 \equiv 0(\text{mod } m), x_2 \equiv 0(\text{mod } m), \cdots, x_n \equiv 0(\text{mod } m)$ as a solution. This solution is called the ***trivial solution***; if there are other solutions, they are called ***nontrivial solution***. Because a homogeneous linear system of congruence always has the trivial solution, there are only two possibilities for its solutions:

- The system of linear congruence has only the trivial solution.
- The system of linear congruence has finitely many solution in addition to the trivial solution

Example 4.7.1.

Solve the homogeneous linear system of congruence

$$\begin{aligned}2x+5y+6z &\equiv 0 \pmod 7\\ 2x \qquad + z &\equiv 0 \pmod 7\\ x+2y+3z &\equiv 0 \pmod 7\end{aligned}$$

Solution

We solved by using Gauss-Jordan elimination

The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 2 & 5 & 6 & \vdots & 0 \\ 2 & 0 & 1 & \vdots & 0 \\ 1 & 2 & 3 & \vdots & 0 \end{bmatrix} \pmod 7.$$

Reducing this modular matrix to reduced row-echelon modulo 7 form

$$\begin{bmatrix} 1 & 0 & 0 & \vdots & 0 \\ 0 & 1 & 0 & \vdots & 0 \\ 0 & 0 & 1 & \vdots & 0 \end{bmatrix} \pmod 7$$

The system of linear congruence has only the trivial solution. Such that:

$$\begin{aligned} x &\equiv 0 \pmod 7\\ y &\equiv 0 \pmod 7\\ z &\equiv 0 \pmod 7\end{aligned}$$

Example 4.7.2.

Solve the homogeneous linear system of congruence

$$\begin{aligned} x+3y+\ \ z &\equiv 0(\mathrm{mod}\,5)\\ x+\ \ y+4z &\equiv 0(\mathrm{mod}\,5)\\ 3x+\ \ y\qquad &\equiv 0(\mathrm{mod}\,5)\end{aligned}$$

Solution

By using Gauss-Jordan elimination method we have

The augmented modular matrix of this system of linear congruence is

$$\begin{bmatrix} 1 & 3 & 1 & \vdots & 0 \\ 1 & 1 & 4 & \vdots & 0 \\ 3 & 1 & 0 & \vdots & 0 \end{bmatrix}(\mathrm{mod}\,5)$$

Reducing this modular matrix to reduced row-echelon modulo 5 form

$$\begin{bmatrix} 1 & 0 & 3 & \vdots & 0 \\ 0 & 1 & 1 & \vdots & 0 \\ 0 & 0 & 0 & \vdots & 0 \end{bmatrix}(\mathrm{mod}\,5).$$

The corresponding system of linear congruence is

$$\begin{aligned} x\qquad +3z &\equiv 0(\mathrm{mod}\,5),\\ y+\ \ z &\equiv 0(\mathrm{mod}\,5).\end{aligned}$$

Solving for the leading variable, we obtain

$$\begin{aligned} x &\equiv 2z(\mathrm{mod}5),\\ y &\equiv 4z(\mathrm{mod}5).\end{aligned}$$

Now, if we assign the free variable z arbitrary value t in Z_5, the *general solution* is given by the formulas

$$\begin{aligned} x &\equiv 2t(\mathrm{mod}\,5)\\ y &\equiv 4t(\mathrm{mod}\,5)\\ z &\equiv \ \ t(\mathrm{mod}\,5)\end{aligned}$$

Note that the trivial solution results when t $\equiv 0(\mathrm{mod}\,5)$.

Reference

1- C.F. Gauss. Disquisitiones Arithmetical Translated by A. A. Clarker Revised by W. C. Waterhourse. New york: Springar-verlag,1986.

2- Number theory with computer applications by R.Kumanduri and C.Romero, Prentice-Hall, Upper Saddle River, New Jersey, 07458

3- W. Adams and L. J. Goldstein, Introduction to Number Theory, Prentice-Hall, Englewood Cliffs, New Jersey, 1976.

4- Kenneth H. Rosen, Elementary Number Theory and lts Applications, ADDISON-WESLEY PUBLISHING COMPANY, 1986.

5- HOWARD ANTON, CHRIS RORRES, Elementary linear algebra , wiley 2010